APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/323,415	06/01/1999	LARRY T. HARADA	06975/041001	9156

26171   7590   01/15/2003

FISH & RICHARDSON P.C.
1425 K STREET, N.W.
11TH FLOOR
WASHINGTON, DC 20005-3500

EXAMINER
NOBAHAR, ABDULHAKIM

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 01/15/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 07-01)

	Application No.	**Applicant(s)**
Office Action Summary	09/323,415	HARADA ET AL.
	Examiner	**Art Unit**	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4)☐ Interview Summary (PTO-413) Paper No(s). _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: .

Response to Remarks

In response to amendment received on 15 November 2002, please note the following:

1.   The changes applied to the specification as suggested by the applicant on pages 1 and 2 of the amendment, are acknowledged.

2.   The minor changes to the claims 13-19 that do not introduce new matter are acknowledged.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3.   The new amended claim 31 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Response to Arguments

Applicant's arguments received on 15 November 2002 have been fully considered but they are not persuasive.

4.   With respect to claims 1 and 22, applicant on page 6, lines 23-24 argues that

"Pepe and Gabber, either alone or in combination, do not describe or suggest these

elements of Applicant's claims 1 and 22", on page 7, line 6 argues that "the client

request of Pepe is not encrypted" and on page 7, lines 16-18, argues that Gabber does

not describe "encrypting profile information; augmenting the data request to target

server."

Due to the open nature (un-trusted) of the WWW (Internet), it would be futile to

transmit the client request to the remote proxy server at the target server location

without encryption. However, Pepe discloses (col. 4, lines 41-44, col. 5, lines 32-39, col.

9, lines 13-16, col. 9, lines 33-41, col. 9, lines 52-55, col. 11, lines 50-54 and Fig. 5) that

the local proxy does encrypt the client request and then transmits it to the target web

server. The user request is decrypted at the remote proxy server and delivered to the

target web server to provide a response for the user.

Gabber discloses (abstract, lines 17-20, page 20, lines 1-7 and page 26,

Requirement 7) that the proxy sever generates an alias for each user accessing a

particular web site that corresponds to the recited user profile and establishes an

account for the user on the information server (page 21, line 19). On the subsequent

visits of the user to the web site (page 24, lines 6-10, page 25, lines 14-15), the user

only inputs a user ID and a password at the beginning of each session to authenticate

himself to the proxy server. The proxy server transmits to the web server the generated

user alias (profile) associated with the user ID and password (page 25, lines 19-21)

along with the user request (page 21, lines 12-17) that corresponds to the recited augmentation of the user request with the user profile. The web server also maintains (page 26, lines 2-3) a list of registered usernames (aliases) at the site.

Examiner contends that a person of ordinary skill in the art would be motivated to combine the teaching of augmenting the user request to a web site with the user alias (corresponding to the recited user profile) generated by the proxy server as taught in Gabber with the method of Pepe because it would provide for secure transmission of the augmented user request to the web server, i.e., encrypted user alias (user profile) be added to the user request at the proxy server then transmitted to the target server.

5.   Regarding claim 4, applicant on page 7, lines 28-30, argues that Gabber "does not send user information to the target web server" and Gabber "does not store user information." Also regarding claim 28, applicant on page 8, lines 14-15 argues that "Pepe and Gabber, either alone or in combination, do not describe or suggest these elements of Applicant's claims 1 and 28" and further he argues that the proxy server in neither Pepe nor Gabber includes a database of user profile information.

As stated above in section 4, the proxy server of Gabber generates an alias for the user based on the user information that is corresponding to the recited user profile that is also based on the user information. The web sever of the Gabber as stated above maintains a list of the user aliases that compare with the received user alias on the subsequent visits of the user to the site. Gabber (page 26, lines 35-36) discloses that the proxy sever has the user private information during a session of interaction but

does not maintain (page 26, lines 37-40) in memory any user information (i.e., a

database or a list of user alias) when the user is not interacting with a web site because

it would prevent the compromise of the users information. Thus, it is apparent that the

issue of not storing the user information on the Gabber proxy server has been a matter

of security.

Examiner contends that a person of ordinary skill in the art would be motivated to

maintain a secured (encrypted) database or a list of users aliases on the proxy server

as Gabber provides it on the web server (page 26, line 3) because the proxy server

would retrieve the user alias from the list instead of re-computing the user alias on

subsequent visits of the user to the web site (page 24, lines 6-10). This would provide

for a faster access to the target web server by the users especially in the case of a large

number of users who are accessing the web server via the same proxy server.

6.   With regard to the applicant argument on page 8, lines 5-6 concerning claims 11

and 12, these claims are rejected as being dependent upon a rejected base claim 1.

Furthermore, Pepe (Fig. 5, items 54 and 68) discloses that the client computer uses a

web browser application and the target server is a web server, i.e., a HTTP server.

Thus, the communications between the client computer and the web server are based

on the hypertext transfer protocol (col. 2, lines 26-37).

7.   With regard to claims 2, 3, 5, 23 and 29 that are dependent upon rejected claims

1, 4, 22 and 28, applicant on page 9, lines 3-4 argues that "White does not remedy any

of the deficiencies of Pepe or Gabber that are noted above with respect to claims 1, 22 and 28."

In addition to the reasons given above in sections 4 and 5 for the rejection of claims 1, 4, 22 and 28, White discloses (Fig. 4) that once the user is authorized to access a web site the web server CGI creates an authentication token (block 112) for the user based on the user information (alias or profile) and sends the token along with the requested results to the client. The client computer stores the authentication token and transmits a copy of the token to the web server with the subsequent requests instead of sending user profile or alias. The web server uses the token to authenticate the user for accessing the information stored on the target web server.

Examiner contends that a person of ordinary skill in the art would be motivated to combine the teaching of using an authentication token as taught in White with the Pepe in view of Gabber because it would provide for the proxy server to append the subsequent user requests with the encrypted token not the user alias or profile.

8.   With respect to claims 13, 25 and 31, applicant on page 9, lines 27-28 argues that "Pepe and Peticolas, either alone or in combination, do not describe or suggest at least these elements of Applicant's claims 13, 25, and 31." Applicant, also, on page 10, lines 3-4 argues that "however, as in Pepe, Peticolas does not describe augmenting a data request with encrypted user profile information."

As stated above in section 4, the proxy server of Pepe encrypts the user request before transmitting it to the target web server but the proxy server does not augment the

user request with any encrypted user information. The user request is decrypted at the remote proxy server and delivered to the target web server to provide a response for the user.

Also, as stated above in section 4, the proxy server of Gabber generates an alias for the user corresponding to the recited user profile and transmits it to the web server along with the user request that corresponds to the recited augmentation of the user request. The web server provides a response for the user (or allow access to the resources) based on the user alias received from the proxy server.

Peticoclas discloses (page 302, section 4.1, line 11) that when the user request is being transmitted from the client side secure proxy (CSSP) to the server side secure proxy (SSSP), other information such as number 3 (a step number), Cp (client address), Sp (web server address) and Ns (a nonce) are added (augmented) to the request and encrypted with a session key (page 303, left column, lines 12-15). At the SSSP the user request is extracted and delivered to the information server. The information server sends back a reply to the SSSP.

Though, Pepe and Peticolas describe a split proxy system including a client-side proxy and the server-side proxy, one skill in the art knows that these proxy servers can be on the client computer and the web server, respectively. Thus, the physical separation of the proxy server from the web server or from the client computer is a matter of choice and would not change the nature of a secure communication between a client and information sever.

Examiner contends that a person of ordinary skill in the art would be motivated to combine the teachings of Peticolas and Gabber with Pepe because it would provide a system in which the proxy server would augment the user request with the encrypted user alias as taught in both Peticolas and Gabber and maintain a database of the users aliases as stated above, in section 5, on the proxy server to be used on the subsequent visits of user to the web site in order to provide a faster user access to the web server. Furthermore, examiner contends that the combined Pepe and Peticolas would establish a *prima facie* case of obviousness with regard to claims 13, 25, and 31.

9.   Claims 14, 15, 18, 27 and 32 are rejected as being dependent on rejected claims 13, 25 and 31, respectively, which they have been rejected in section 8, above.

10.   With regard to applicant's argument on page 10, lines 12-17, claims 16, 17, 19-21 and 26 that are dependent on rejected claims 13 and 25, respectively, are rejected based on the reasons given above, in sections 7 and 8.

Examiner contends that the combination of Pepe, Peticolas and White establishes a *prima facie* case of obviousness with regard to claims 16, 17, 19-21 and 26.

11.   However, based on the above submission, examiner maintains the previous rejection.

12.   Applicant on pages 3-5 has introduced new claims 33-42. However, these claims

do not add any new matter to the previous claims and are rejected over Pepe in view of

Gabber and Lincke as applied to like elements of claims 1-32 and the following.

Pepe (col. 6, lines 59-63), Gabber (page 21, lines 1-19) and Lincke (col. 2, lines

5-10) disclose the use of HTTP protocol over the TCP connection for communication

between the computer client and the information (web) server. As stated above in

sections 4 and 5, the client request is routed through a proxy server to the information

server. The proxy server determines the target (destination) web server based on the

HTTP request receives from the client. Particularly, as stated above in section 4, the

proxy server of Gabber generates a specific user alias for each web server that requires

the user to be authenticated for accessing restricted or secured resources. Every time

the user attempts to visit a web site, the proxy sever sends the relevant alias to the

targeted web site along with the user request if the target server requires the user to be

authenticated

Linke (col. 3, lines 38-59) discloses a method of using a data encryption

(session) key and the use of the server's public key for securely transmitting a message

from a client to a server. The client encrypts the message using the data encryption key

and encrypts the data encryption key using the public key of the server and then

transmits the encrypted message to the server. The server recovers the data encryption

key using the server private key corresponding to the server public key. The server uses

the data encryption key to decrypt the encrypted request message and to encrypt the

response message before transmitting it to the client.

Examiner, however, contends that a person of ordinary skill in the art would be

motivated to combine the above teachings of Lincke with Pepe in view of Gabber

because it would provide for secure transmission of messages between the client

computer and the web server.

Previous Rejection:

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

14. Claims1, 4, 11, 12, 22, and 28 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Pepe et al. (5,673,322) (hereinafter Pepe) in view of Gabber et

al. (XP-002059819) (hereinafter Gabber).

15. As per claims 1, 11, and 22, Pepe (Figure 5) discloses a client using a web browser

54 to send a request to a web sever 68 via a local proxy sever 56. The proxy server

56 converts it from an application layer protocol based message to a transport layer

protocol based message (column 5, lines 54 through 56), then transmits the

request to a remote proxy server (column 11, line 55), located at the target web

server place (column 5, lines 50 through 52). Also, Pepe (column 14, lines 25

through 35) discloses the conversion process includes encrypting the client

request, and further indicates (column 9, lines 13 through 40) that for this purpose,

one of ordinary skill in the art could easily design an encryption scheme based on

well-known principles. Pepe, however, does not specifically disclose the

augmentation of the user request with encrypted user profile information and its

transmission directly to the web server. Gabber teaches the implementation of a

cryptographic function and transmission of the user request directly to a targeted

web server by a proxy server named Janus (page 20, lines 4 through 7 and page

21, lines 12 through 13). Gabber also teaches appending the user request with new

information related to the user before sending it to the web server (page21, line 23

and page 24, lines 1 through 5). It would have been obvious to one of ordinary skill

in the art at the time the invention was made to append a user request with new

information related to the user before sending it to the web server as taught in

Gabber in the communication systm of Pepe because it would provide for the

secure and direct access of the user to the targeted web site. This arrangement

especially is advantageous for the web sites that do not have external proxy sever.

16. As per claim 4, 12 and 28, Pepe does not disclose the retrieval of user profile

information from a database. Gabber teaches the use of user information by the

proxy server to be sent along with the user request to the web server. This is

indicative of retrieving the user information from a kind of storage, i.e. a database

containing user information (page 21, paragraph 3). It would have been obvious to

one of ordinary skill in the art at the time the invention was made to combine the

teaching of Pepe with Gabber because it would provide for the proxy server to carry

out only the process of authentication of the user on the subsequent visits of the

user to the web site.

17. Claims 2, 3 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Pepe et al. (5,673,322) (hereinafter Pepe) in view of Gabber et al. (XP-002059819)

(hereinafter Gabber) and further in view of White (6,049,877).

18. Pepe in view of Gabber teaches all the limitations of the above claims but does not

specify the creation of a token in reference to the user information by the web

server to be transmitted to the client proxy server. White, however, teaches that the

web server creates a token with regard to the user information. The token is sent to

and being stored at the client proxy server for use with subsequent user requests

(column 10, lines 1 through 11). It would have been obvious to one of ordinary skill

in the art at the time the invention was made to create a token for subsequent user

request as taught in White, in the system of Pepe in view of Gabber because it

would allow a proxy sever not to encrypt and transmit the user information profile in

the subsequent queries to the web server by the user.

19. Claims 6-10, 24 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pepe et al. (5,673,322) (hereinafter Pepe) in view of Gabber et al. (XP-002059819) (hereinafter Gabber) and further in view of Lincke et al. (6,253,326 B1) (herinafter Lincke.)

20. Pepe discloses the use of an encryption scheme for encrypting the user request (column 14, line 31). Pepe in view of Gabber does not specify the method of the encryption. Lincke teaches the generation and the use of a local key as an encryption key to encrypt the user message and the use of a public key to encrypt the local key (column 115, lines 45 through 55). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a local key as encryption key as taught in Lincke for the encryption system of Pepe in view of Gabber because it would provide for the proxy sever to securely transmit the encryption key to a remote web server site.

21. Claims 13-15, 18, 25, 27, 31, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pepe et al. (5,673,322) (hereinafter Pepe) in view of Petitcolas (XP-00214286).

22. As per claim 13-15, 18, 25, 27, 31, and 32, Pepe discloses creation of a response to user request at the targeted web site server and transmitting it to the client proxy server (column 16, lines 1 through 12). Pepe, however, does not specify the extraction of user information from the request in order to generate a response.

Petitcolas teaches the extraction of user information from the receiving message and using this information to generate a response and transmitting it back to the client proxy (page 302, section 4.1). It would have been obvious to one of ordinary skill in the art at the time the invention was made to extract the user information from the user request at the information server as taught in Petitcolas in the system of Pepe, because it would allow the information server to generate a response for the user and transmit it to the client proxy server without further re-transmission of user information back and forth between the client site and the web site, thus reducing the magnitude of the encryption process and the transmitting messages between the two sites.

23. Claims 16,17, 19-21, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pepe et al. (5,673,322) (hereinafter Pepe) in view of Petitcolas (XP-00214286) and further in view of White (6,049,877).

24. As per claim 16, 17, 19-21, and 26, Pepe in view of Petitcolas discloses all the limitations of these claims but does not specify associating a reference token with the user information and including it in the response. White, however, teaches associating a token with the user information and transmitting the token with response to the client proxy server (column 10, lines 1 through 24). It would have been obvious to one of ordinary skill in the art at the time the invention was made to create a token at the information server to be sent to the client proxy for use with

subsequent user request as taught in White, in the system of Pepe in view of

Petitcolas, because it would allow the information server to generate a token in

association with the user, and transmit to the client proxy server only the token

along with the response for use with the subsequent requests. This combination

eliminates the transmission of user information back to the client site, thus reducing

the magnitude of the encryption process and the transmitting message to the client

proxy.

25. Claims 23, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Pepe et al. (5,673,322) (hereinafter Pepe) in view of Gabber and further in view of

White (6,049,877).

26. As per claim 23 and 29, Pepe in view of Gabber discloses all the limitations of

these claims, but does not specify the generation of a reference token at the web

server for use with the subsequent user requests. White, however, teaches the use

of a token with the subsequent user requests to be transmitted to the web server

(column 10, lines 1 through 24). It would have been obvious to one of ordinary skill

in the art at the time the invention was made to create a token in reference to the

user at the information server as taught in White in the system of Pepe in view of

Gabber, because it would allow the proxy server to transmit only the reference

token along with the subsequent user requests to the information server. This

combination eliminates the re-transmission of user information from the user site to

the web site, thus reducing the magnitude of the transmitting messages to the web

site by the proxy server.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-

305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone numbers

for the organization where this application or proceeding is assigned are 703-746-7239

for regular communications and 703-746-7238 for After Final communications.
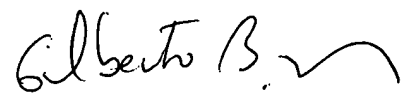
Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist whose telephone number is 703-305-3900.

Abdulhakim Nobahar

January 9, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100